DEUSOP16 - Software/Hardware Validations, Verifications, Maintenance and Performance Checks

Table of Contents

1. Scope

1.1. This standard operating procedure addresses how the DEU will validate, performance check and maintain the in-service hardware and software.

2. Background

2.1. To establish the practices for documenting the examination of evidence to conform to the requirements of the Department of Forensic Sciences (DFS) Digital Evidence Unit *Quality Assurance Manual*, the accreditation standards under ISO/IEC 17025:2017, and any supplemental standards.

3. Safety

3.1. If necessary for the validation/performance check or maintenance of the hardware or software, wear personal protective equipment (PPE) while performing procedures.

4. Materials Required

4.1. Hardware and software to be performance checked/validated; other validated forensic tools; DEU Reference Sets/NIST created testing images.

5. Standards and Controls

5.1. Not applicable.

6. Calibration

6.1. Not applicable.

7. Procedures

7.1. Software Validation/Verification

7.1.1. All software that is used by the DEU must be tested to ensure that the software performs its functions successfully. Testing is done with known data sets that produce expected results and recorded on DEUF10 – Software Validation and saved with equipment maintenance records.

7.1.2. If a standards creating body (e.g. NIST) has formally tested and validated the software used by DEU, DEU will perform a "performance check" to ensure the software is working correctly, which will be documented on DEUF10 – Software Validation to be saved with equipment maintenance records.

7.1.3. Software that has been validated and verified by another ISO/IEC 17025 accredited laboratory can be used by the DEU, documenting the laboratory that has previously validated the software on DEUF10 – Software Validation to be saved with the equipment maintenance records.

7.1.4. All functions of a piece of forensic software may not be validated/performance checked. Only the functions used by and pertinent to the DEU per piece of software will be validated/performance checked and reported.

7.1.5. For all software used in the DEU, only major migrations or version releases will be validated/performance checked. A release is considered a major release if the versioning number has changed. Example: Software v 1.1.1 to Software v 2.0.0.

7.1.5.1. An example of a non-major release is Software v 1.2.3.4.5 to Software v 1.2.3.4.6. These will not be performance checked/validated in the DEU.

7.1.6. For all non-major releases, the release notes will be read and, if not accessible on the vendor's website, will be saved to the DEU shared drive.

7.1.7. Once the software has been tested, it will be added to the DEU Approved Software/Hardware List with the version and the date it was added.

7.2. Hardware Validation/Verification

7.2.1. All hardware that is used by the DEU must be tested to ensure that the hardware performs its functions successfully. Testing is done with known data sets that produce expected results and recorded on DEUF14 – Hardware Validation and saved with equipment maintenance records.

7.2.2. DEU does not performance check/test/validate/verify chip-off/JTAG/ISP equipment unless a known readable chip is available. Checking this equipment requires destruction or potential destruction of a device in order to test.

7.2.3. If a standards creating body (e.g. NIST) has formally tested and validated the hardware used by DEU, DEU will perform a "performance check" to ensure the software is working correctly, which will be documented on DEUF14 – Hardware Validation to be saved with equipment maintenance records.

7.2.4. Hardware that has been validated and verified by another ISO/IEC 17025 accredited laboratory can be used by the DEU, documenting the laboratory that has previously validated the software on DEUF14 – Hardware Validation to be saved with equipment maintenance records.

7.2.5. All functions a piece of forensic hardware has may not be validated/performance checked. Only the functions used by and pertinent to the DEU will be validated/performance checked and reported.

7.2.6. For all hardware used in the DEU, only major migrations or version releases will be validated/performance checked. A release is considered a major release if the versioning number has changed. Example: Hardware v1.1.1 to Hardware v2.0.0.

7.2.6.1. For all non-major releases, the release notes will be read and, if not accessible on the vendor's website, will be saved to the DEU Shared drive.

7.2.7. For all firmware upgrades, hardware will be performance checked once the firmware upgrade is completed. This will be recorded on the DEUF14 – Hardware Validation and saved with equipment maintenance records.

7.2.8. Once the hardware has been validated/verified, it will be added to the DEU Approved Software/Hardware List with the version and the date it was added.

7.3. Writeblocker Verification/Maintenance

7.3.1. All writeblockers within the DEU will be validated/performance checked using known DEU Data sets.

7.3.2. DEU writeblockers will be annually performance checked and the results recorded on DEUF13 – Writeblocker Verification Checklist.

7.3.3. All recorded results will be kept with the DEU equipment maintenance logs.

7.3.4. Once a writeblocker has been initially validated/performance checked, it will be added to the DEU Approved Software/Hardware List.

7.4. DEU Maintenance Log

7.4.1. All activities regarding DEU hardware will be noted on each item's log, which is maintained as part of the equipment records.

7.5. DEU Forensic Workstations/Laptops

7.5.1. DEU Forensic Workstations are Windows or Apple platforms that run the performance checked/verified/validated hardware and software. A satisfactory performance check is achieved when the workstations successfully "POST" (Power On Self Test) at start up. Forensic Workstations are not verified/validated like forensic hardware or software but are put into service and tracked via individual maintenance logs.

7.5.2. DEU Forensic Workstations that do not POST will be taken out of service and not used for forensic examination.

7.5.3. DEU Forensic Workstations are not connected to an Internet network and access is controlled via the DEUNet Active Directory.

7.5.4. DEU Laptops are Internet connected and are used primarily for research, downloading updates/releases, administrative communications (email) and DEU business.

7.5.5. When forensic software requires Internet access, the software is loaded on to the laptop and is the only forensic software used on the laptop. A DEU desktop computer may also be connected to the Internet if required for forensic software. This computer cannot be reconnected to DEUnet once it has connected to the Internet, unless the internal drive(s) have been wiped and reimaged.

8. Sampling

8.1. Not applicable.

9. Calculations

9.1. Not applicable.

10. Uncertainty of Measurement

10.1. Not applicable.

11. Limitations

11.1. Not applicable.

12. Documentation

12.1. DEUF10 – Software Validation

12.2. DEUF12 – Equipment Maintenance Log

12.3. DEUF13 – Writeblocker Verification Checklist

12.4. DEUF14 – Hardware Validation

12.5. DEU Approved Software/Hardware List

13. References

13.1. Digital Evidence Unit Quality Assurance Manual (Current Version).

13.2. DFS Departmental Operations Manuals (Current Versions).

13.3. Forensic Science Laboratory (FSL) Laboratory Operations Manuals (Current Versions).

13.4. Digital Evidence Unit Laboratory Operations Manuals (Current Versions).

13.5. SWGDE Recommended Guidelines for Validation Testing (v2.0 September 5, 2014).